

Coding Centre

The problem

- Government has many registers with information about people
- Registers have two uses
 - Everyday use (operative data)
 - Research use (statistics)

The problem (2)

- Some registers contain highly sensitive information
- Even belonging to registry can be sensitive
 - Examples: AIDS register, drug treatment register

The problem (3)

- Research often requires linking of several registries
 - For example, mobile phones and cancer, HIV and drug treatment

Drug treatment register

- Information about drug rehabilitation treatments is stored in hospitals
 - Personalized data for everyday operation
- Hospitals send data to drug treatment register that aggregates data and allows people to do research
- Researchers must apply for permit to perform specific queries against that data

What are the risks?
How to mitigate them?

The law

- EU: processing sensitive personal data without consent is allowed for scientific purposes
- Scandinavia: the same
- Estonia: processing sensitive personal data is allowed only for saving person's life or for purposes allowed by other laws

The law (2)

- Drug treatment database is kept in a form that does not allow identifying persons registered in the database

Official threat model

- The organization that runs the database cannot be trusted
- Alternatively: research data is operated using lower security measures

How to mitigate this threat?

Simple coding centre

- Separate from hospitals and drug register
- Contains key K
- Encrypts person ID codes using this key
- Registry stores encrypted ID codes

Attacks on this scheme?
What can be improved?